American Medical Informatics Association
The professional home for biomedical and health informatics

October 22, 2009

U.S. Department of Health and Human Services
Office for Civil Rights
Attention: HITECH Breach Notification
Hubert H. Humphrey Building
Room 509 F
200 Independence Avenue, SW
Washington, DC 20201

45 CFR PARTS 160 and 164

RIN: 0991-AB56
Breach Notification for Unsecured Protected Health Information
Interim final rule with request for comments

Dear Secretary Sebelius:

On behalf of the American Medical Informatics Association (AMIA) I am pleased to submit these comments in response to your request for public input to the above reference proposed final rule. AMIA is the professional home for biomedical and health informatics and is dedicated to the development and application of informatics in support of patient care, public health, teaching, research, administration, and related policy. AMIA seeks to enhance health and healthcare use through the transformative use of information and communications technology.

AMIA's 4,000 members advance the use of health information and communications technology in clinical care and clinical research, personal health management, public health/population, and translational science with the ultimate objective of improving health. Our members work throughout the health system in various clinical care, research, academic, government, and commercial organizations.

As a source of informed, unbiased opinions on policy issues relating to the national health information infrastructure, uses and protection of clinical and personal health information, and public health considerations, we appreciate the opportunity to submit comments on the above-referenced guidance and request for information.

AMIA thanks the Department for issuing in timely fashion this Interim Final Rule, which implements Section 13402 of the American Recovery and Reinvestment Act (ARRA) (Pub. L. 111-5) while also providing guidance "specifying technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals". Having previously provided

4915 St. Elmo Avenue, Suite 401 ▫ Bethesda, MD 20814
Phone 301.657.1291 ▫ Fax 301.657.1296
E-mail: mail@amia.org ▫ www.amia.org

extensive comments to the draft version of the Guidance, and responded as well to the Request for Information regarding the breach notification provisions of ARRA, we will first review several clarifications offered by the Department regarding the Guidance and then proceed to a discussion of selected provisions of the Interim Final Rule.

The Guidance

Section 13402 of ARRA requires breach notification following the discovery of a breach of unsecured PHI, which is defined as PHI "that is not secured through the use of a technology or methodology specified by the Secretary". In this Guidance the Department clarifies that covered entities (CEs) and business associates (BAs) are not required to use the technologies and methodologies that are specified for rendering PHI "not unsecured" – encryption and destruction – in order to comply with the HIPAA Security Rule (45 CFR, part 164, subparts A and C). Rather, the CE or BA may use other methods, such as firewalls and access controls, to address the reasonable, appropriate and scalable implementation specifications of the Security Rule. AMIA appreciates the distinction drawn between the range of methods that may be used to make information inaccessible for purposes of complying with the Security Rule versus the two methods – encryption and destruction – the Department recognizes as sufficient for meeting the higher statutory standard of rendering PHI "unusable, unreadable, or indecipherable to unauthorized individuals" and thereby exempt from breach notification requirements. The Guidance helpfully provides additional information on NIST publications relating to encryption technologies and processes for data storage and data in motion. We thank the Department for including in the Guidance a security measure previously suggested by AMIA: that encryption keys should be kept on a separate device from the data that they encrypt or decrypt.

In articulating methods for rendering health information 'not unsecured' and thereby exempt from breach reporting, we are concerned that some may perceive that the Department has effectively established a *de facto* 'standard of care' for "data in motion" and "data at rest". While more sophisticated CEs and BAs may be able to make extensive use of encryption, AMIA wonders about the capability of many covered entities, such as small physician practices or small clinics, to meet such a standard. As we do not believe that it is the Department's intention to "require" encryption, as indicated by the Guidance's careful discussion of alternate methods for complying with the Security Rule, AMIA requests that future revisions to this Guidance contain a specific statement that encryption has not, at this time, been established as a 'standard' for the storage or transmission of protected health information by covered entities or business associates.

The Interim Final Rule – Selected Provisions

As defined by ARRA, *breach* means the acquisition, access, use, or disclosure of PHI which compromises the security or privacy [emphasis added] of the PHI. The Rule (at § 164.502) further elaborates on the meaning of "compromises" security or privacy, noting that "For purposes of this definition, compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm [emphasis added] to the individual." AMIA

supports this definition, that operationalizes the statutory direction that a breach must "compromise" security or privacy in some meaningful way. By requiring CEs and BAs to exercise judgment in assessing the risk posed by a breach, the Rule aligns federal breach reporting requirements with those of most state laws and will serve to protect individual privacy by encouraging responsible information security practices rather than reliance on pro forma notifications of breaches to individuals who, if a significant risk of harm has not occurred, have no practical steps to take toward remedying a non-existent harm.

Even as the Interim Final Rule incorporates a risk of harm threshold for breach reporting, it substantially increases the obligations of HIPAA covered entities and business associates. Health care entities must establish programs to monitor for and detect breaches, establish processes to evaluate whether a breach poses a significant financial, reputational, or other harm to individuals, document risk assessment processes and results, and determine when providing notice to individuals, the Department and the media is required. Such actions will strengthen consumer trust in health care organizations and provide meaningful, actionable information to individuals. By contrast, notification of individuals when there is not significant risk of harm would engender unnecessary concern at best, and 'notice fatigue' at worst.

Some may suggest that providing a measure of discretion to CEs and BAs for determining whether a harm standard has been met will lead to HIPAA covered entities failing to provide notifications to individuals when a meaningful breach has occurred – we strongly disagree that this will be the result. In fact, absent clearer guidance for determining what constitutes a "significant risk of financial, reputational, or other harm to the individual", we believe it far more likely that risk-averse covered entities and business associates will over-report possible breaches. (The negative impact of the current HIPAA Privacy Rule on research supports the idea that CEs are unlikely to exercise the level of discretion afforded to them. AMIA commends to the Department the Institute of Medicine (IOM Report) "Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health through Research" for a fuller discussion of the need for a balance between privacy and necessary research.) Related to the question of making a determination as to whether a breach "compromises the security or privacy of protected health information," AMIA suggests that the Department continue and extend the very useful discussion begun in the Interim Final Rule of factors to be considered in assessing "risk of financial, reputational, or other harm" with additional Guidance or other communications, such as an FAQ on the topic.

In discussing the definition of *breach* the Interim Final Rule clarifies that an "unauthorized" acquisition, access, use, or disclosure of PHI is one that is not permitted by the Privacy Rule. We support this clarification, as well as the corollary statement that not all violations of the Privacy or Security Rules will constitute breaches or trigger notification obligations. This provides a clear roadmap that when a CE or BA discovers a use or disclosure in violation of the Privacy Rule, it should then determine whether such use or disclosure "compromises the security or privacy" of the PHI. However, this section also raises the possibility that a violation of the *minimum necessary* requirement of the Privacy Rule could trigger notification; again, we recommend that the Secretary consider adding a corollary statement that neither minimum necessary use violations, which typically occur within the CE, nor minimum

necessary disclosure violations, if made as permitted to another CE or BA similarly covered by the Privacy and Security Rules, would be likely to trigger notification. We suggest, then, that further discussion of the interaction between minimum necessary and breach reporting requirements be taken up in a separate Guidance regarding what constitutes "minimum necessary" as called for at Sec. 13405 (b)(1)(B) of ARRA.

For reasons outlined at length in our comment to the previous draft Guidance and Request for Information, AMIA continues to believe that the breach notification requirements imposed on CEs and BAs by this Interim Final Rule should not apply to limited data sets (LDS), as the "acquisition, access, use, or disclosure" of an LDS in a manner not permitted by the Privacy Rule is, simply, highly unlikely to pose "a significant risk of financial, reputational, or other harm to the individual." With direct identifiers removed, a data use agreement in place and, as we suggested, a requirement that decryption keys be maintained separately from the data set, we believe that the privacy and security risks involved in re-identifying the unique individuals for whom a single data element (e.g., date of hospital discharge) was included in an LDS will greatly outweigh any benefit of notification, which would provide no useful or actionable information to the individual.

While we appreciate that the Department has decided (at § 164.402 (1)(ii)) that an LDS that does not include date of birth and zip code does not compromise the security or privacy of PHI and thus is excluded from the definition of breach, AMIA is concerned that this 'redefinition' of limited data sets will actually result in less availability of data sets for important research. Extending our request for additional guidance, perhaps in the form of an FAQ, we would suggest that the Department clarify that when performing a risk assessment relating to a potential 'breach' of a limited data set, a CE should presume that such a non-permitted use or disclosure will not involve a significant risk of harm absent specific and compelling evidence to the contrary.

AMIA supports the exclusions to the definition of breach outlined in § 164.402 (2). We would suggest that § 164.402 (2)(ii) should be amended to read: "any inadvertent disclosure by a person… to another person authorized to access protected health information at the same **or another** covered entity or business associate… and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted…" Simply, we believe that inadvertent disclosures to other entities that are covered by the Privacy and Security Rules will not result in a significant risk of harm to individuals and therefore should be excluded from the definition of breach. In fact, the discussion suggests that a reporting obligation would not attach to such an inadvertent disclosure "unless the information is [then] breached while at the third party [if the third party is itself a covered entity] and it is then the third party that "will be responsible for complying with the provisions of this interim final rule." (On a related note, we appreciate the clarification that "a covered entity or business associate is not responsible for a breach by a third party to whom it permissibly disclosed protected health information, including limited data sets, unless the third party received the information in its role as an agent of the covered entity or business associate.")

In our previous comment to the draft Guidance and RFI, AMIA noted that:

A comprehensive health record is likely to contain PHI gathered from many covered entities – in fact, this is one of the principal functions of an HIE or RHIO, to facilitate access to the many records that relate to the same individual… If there were an instance in which a RHIO (a BA) suffered a breach of PHI relating to one or more individuals, that RHIO would, presumably, need to notify all of the CEs that 'provided' PHI relating to a given individual – or perhaps even all the CEs with which it has contracts – and each of those CEs would in turn need to send a notice to the individual that his/her unsecured PHI was acquired, accessed, used, or disclosed in a way that compromised the security or privacy of the individual's information. Not only will this result in multiple (and confusing) breach notices being sent to the same individual, but it will put multiple CEs 'on the hook' to disclose how they will prevent such breaches in the future (perhaps by withdrawing from the RHIO or the PHR), advise the individual about steps he/she should take to prevent harm, and the like.

At the time, AMIA requested that the Department provide meaningful guidance concerning the breach reporting obligations of multiple CEs that may 'provide' PHI to a comprehensive record 'through' a RHIO or HIE. Unfortunately, we find the discussion of § 164.410 unhelpful on this point: "Thus, following the discovery of a breach of unsecured protected health information, a business associate is required to notify the covered entity of the breach so that the covered entity can notify affected individuals [emphasis added]… In cases in which a breach involves the unsecured protected health information of multiple covered entities and it is unclear to whom the breached information relates, it may be necessary to notify all potential affected covered entities" – whom, we note, will then be required to send multiple breach notices to the same individual. Unfortunately, we find unhelpful the Department's assertion that, "we believe it appropriate to leave it up to covered entities and business associates to determine how the required reporting should be implemented." Again, AMIA suggests the need for further guidance relating to the reporting obligations of covered entities in such situations.

Concluding Comments

Especially in light of the significant administrative requirements – including but not limited to additional workforce training and sanctions, the establishment of new complaint procedures, and the development of new risk assessment procedures and documentation – (at § 164.530) faced by CEs and BAs in order to comply with this Rule, AMIA appreciates the Department's decision "to not impose sanctions for failure to provide the required notifications for breaches that are discovered before 180 calendar days from the publication of this rule". While covered entities and business associates will, of course, make every effort to comply with the Rule, the opportunity to access advice and technical assistance between now and February 23, 2010 will better support the transition to widespread compliance than would the application of sanctions.

Finally, having noted the burden of new administrative requirements, very significant costs will be incurred to comply with these breach notification requirements. From developing programs to monitor and detect potential breaches and establishing risk assessment procedures (e.g., constituting risk assessment teams,) to training staff, retaining additional legal personnel and developing a range of new

communication channels for consumers, the costs to covered entities will not be trivial. We urge the Department to maintain and extend the common sense balance between privacy protection and return on investment in an already overstressed and extraordinarily expensive health care system that we see in certain provisions of the Interim Final Rule, exemplified best by the inclusion of a harm standard in making a determination regarding a potential breach.

AMIA thanks the Department for issuing this Interim Final Rule and appreciates the opportunity to submit comments. Please feel free to contact me at any time for further discussion of the issues raised here.

Sincerely,

Edward H. Shortliffe, MD, PhD
President and CEO